PTO/SB/17 (08-00)
Approved for use through 10/31/2002 OMB 0651-0032
U S Patent and Trademark Office U S DEPARTMENT OF COMMERCE

FEE TRANSMITTAL for FY 2000

Patent fees are subject to annual revision.

TOTAL AMOUNT OF PAYMENT ($) 1,646.00

Complete if Known	
Application Number	
Filing Date	October 31, 2000
First Named Inventor	Lyndon Ong
Examiner Name	
Group/Art Unit	
Attorney Docket No.	003239.P076

METHOD OF PAYMENT (check one)

1. ☒ The Commissioner is hereby authorized to charge indicated fees and credit any overpayments to:

Deposit Account Number: 02-2666

Deposit Account Name: Blakely, Sokoloff, Taylor & Zafman LLP

☒ Charge Any Additional Fee(s) Required Under 37 CFR §§ 1 16, 1 17, 1 18 and 1 20

☐ Applicant claims small entity status See 37 CFR 1 27

2. ☒ **Payment Enclosed:**

☒ Check ☐ Credit card ☐ Money Order ☐ Other

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
101	710	201	355	Utility filing fee	710.00
106	320	206	160	Design filing fee	
107	490	207	245	Plant filing fee	
108	710	208	355	Reissue filing fee	
114	150	214	75	Provisional filing fee	

SUBTOTAL (1) ($) 710.00

2. EXTRA CLAIM FEES

			Extra Claims		Fee from below		
Total Claims	52	- 20** =	32	X	18.00	=	$576.00
Independent Claims	7	- 3** =	4	X	80.00	=	$320.00
Multiple Dependent						=	

**or number previously paid, if greater, For Reissues, see below

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
103	18	203	9	Claims in excess of 20
102	80	202	40	Independent claims in excess of 3
104	260	204	135	Multiple Dependent claim, if not paid
109	80	209	40	**Reissue independent claims over original patent
110	18	210	9	**Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) 896.00

FEE CALCULATION (continued)

3. ADDITIONAL FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
105	130	205	65	Surcharge - late filing fee or oath	
127	50	227	25	Surcharge - late provisional filing fee or cover sheet.	
139	130	139	130	Non-English specification	
147	2,520	147	2,520	For filing a request for reexamination	
112	920*	112	920*	*Requesting publication of SIR prior to Examiner action	
113	1,840*	113	1,840*	*Requesting publication of SIR after Examiner action	
115	110	215	55	Extension for response within first month	
116	390	216	195	Extension for response within second month	
117	890	217	445	Extension for response within third month	
118	1,390	218	695	Extension for response within fourth month	
128	1,890	228	945	Extension for response within fifth month	
119	310	219	155	Notice of Appeal	
120	310	220	155	Filing a brief in support of an appeal	
121	270	221	135	Request for oral hearing	
138	1,510	138	1510	Petition to institute a public use proceeding	
140	110	240	55	Petition to revive - unavoidable	
141	1,240	241	620	Petition to revive - unintentional	
142	1,240	242	620	Utility issue fee (or reissue)	
143	440	243	220	Design issue fee	
144	600	244	300	Plant issue fee	
122	130	122	130	Petitions to the Commissioner	
123	50	123	50	Petitions related to provisional applications	
126	240	126	240	Submission of Information Disclosure Stmt	
581	40	581	40	Recording each patent assignment per property (times number of properties)	40.00
146	710	246	355	Filing a submission after final rejection (37 CFR § 1.129(a))	
149	710	249	355	For each additional invention to be examined (37 CFR § 1.129(b))	
179	710	126	355	Request for Continued Examination (RCE)	
169	900	169	900	Request for expedited examination of a design application	

Other fee (specify) _____

Other fee (specify) _____

*Reduced by Basic Filing Fee Paid

SUBTOTAL (3) ($) 40.00

SUBMITTED BY

Complete (if applicable)

Name (Print/Type)	Thinh V. Nguyen	Registration No. (Attorney/Agent)	42,034	Telephone	(714) 557-3800
Signature				Date	10/31/00

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2039.

Docket No. 003239.P076
Express Mail No.: EL466330290US

UNITED STATES PATENT APPLICATION

FOR

REAL-TIME MEDIA COMMUNICATION OVER FIREWALLS USING A CONTROL PROTOCOL

INVENTOR:

LYNDON ONG

PREPARED BY:

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
12400 Wilshire Blvd., 7th Floor
Los Angeles, CA 90025-1026
(714) 557-3800

REAL-TIME MEDIA COMMUNICATION OVER FIREWALLS USING A CONTROL PROTOCOL

BACKGROUND

1. Field of the Invention

This invention relates to network communication. In particular, the invention relates to firewalls.

2. Description of Related Art

Currently, firewalls do not admit traffic which is not recognized. Most voice over Internet protocol (VoIP) traffic is not allowed across a firewall boundary because VoIP traffic contains no indication that the packet is VoIP and no indication of the originating and destination parties in the call. This limits VoIP service to service within a firewall-protected domain and does not allow users within the domain to call outside the domain and vice versa.

One existing technique is to add intelligence to firewall protocol so that the firewall can understand call signaling protocol (e.g., H.323) and can determine what Internet protocol (IP) address pair and UDP port pair to admit for a particular call. This technique has a number of drawbacks. First, the firewall is required to have significantly greater processing power and demands, resulting in high costs and integration efforts. Second, the firewall is required to be updated frequently as call signaling protocols change or are introduced, resulting in high maintenance and downtime costs. Third, the signaling is required to be processed by the firewall on every call, adding set-up delays and slowing down traffic.

Therefore, there is a need in the technology to provide an efficient technique for media communication via firewalls.

SUMMARY

The present invention is a method and apparatus to provide real-time media communication via firewalls. A real-time firewall includes a controller, a filter, and a modifier. The controller specifies a filtering characteristic based on a control protocol from a call server serving a firewall between source and a destination networks. The filter filters a packet in a call transmitted from the source network based on the filtering characteristic. The filter accepts the packet if the packet satisfies the filtering characteristic and rejects the packet otherwise.

According to one embodiment of the present invention, the controller further specifies a modifying action based on the control protocol. The real-time firewall further includes a modifier coupled to the controller and the filter to modify the accepted packet based on the modifying action. The modified packet is then sent to the destination network. The filtering characteristic may be at least one of a traffic characteristic, a network address, and a port identifier corresponding to the call.

The firewall in this invention may be able to do at least one of the following: (1) providing extensibility to existing firewall set-up, (2) allowing users within a firewall to call users outside firewall and vice versa, (3) increasing effective traffic management over firewall boundaries, and (4) accommodating real-time media communication over firewalls at low costs.

Other aspects and features of the present invention will become apparent to those ordinarily skilled in the art upon review of the following description of specific embodiments of the invention in conjunction with the accompanying figures.

BRIEF DESCRIPTION OF THE DRAWINGS

The features of the present invention will become apparent from the following detailed description of the present invention in which:

Figure 1 is a diagram illustrating a system in which at least one embodiment of the invention can be practiced.

Figure 2 is a diagram illustrating a real-time firewall according to one embodiment of the invention.

Figure 3 is a flowchart illustrating a process for real-time media communication across firewall according to one embodiment of the invention.

DESCRIPTION

A method and apparatus provides a technique for media communication across a firewall boundary in a network environment. In one embodiment of the invention, a real-time firewall includes a controller, a filter, and a modifier. The controller specifies a filtering characteristic based on a control protocol from a call server serving a firewall between a source and a destination networks. The filter filters a packet in a call transmitted from the source network based on the filtering characteristic. The filter accepts the packet if the packet satisfies the filtering characteristic and rejects the packet otherwise.

The firewall in this invention may be able to do at least one of the following: (1) providing extensibility to existing firewall set-up, (2) allowing users within a firewall to call users outside firewall and vice versa, (3) increasing effective traffic management over firewall boundaries, and (4) accommodating real-time media communication over firewalls at low costs.

In the following description, for purposes of explanation, numerous details are set forth in order to provide a thorough understanding of the present invention. However, it will be apparent to one skilled in the art that these specific details are not required in order to practice the present invention. In other instances, well-known electrical structures and circuits are shown in block diagram form in order not to obscure the present invention. For example, specific details are not provided as to whether the method is implemented in a station as a software routine, hardware circuit, firmware, or a combination thereof.

Embodiments of the invention may be represented as a software product stored on a machine-readable medium (also referred to as a computer-readable medium, a processor-readable medium, or a computer usable medium having a computer readable program code embodied therein). The machine-readable medium may be any type of magnetic, optical, or electrical storage medium including a diskette, compact disk read only memory (CD-ROM), memory device (volatile or non-volatile), or similar storage mechanism. The machine-readable medium may contain various sets of instructions, code sequences, configuration information, or other data. Those of ordinary skill in the art will appreciate that

other instructions and operations necessary to implement the described invention may also be stored on the machine-readable medium. Software running from the machine readable medium may interface with circuitry to perform the described tasks.

Figure 1 is a diagram illustrating a system 100 in which one embodiment of the invention can be practiced. The system 100 includes a public network 110, a private network 170, and a firewall 140.

The public network 110 is a public network external to the organization, e.g., the Internet. The public network 110 includes an end system 120 and a call server 130. The end system 120 is a system that receives or transmits a call or a message. Examples of the end system 120 include a computer, a call processing unit, a workstation, a private branch exchange (PBX), a telephony device, a wireless call unit. The end system 120 sends or receives real-time packets 152 to or from the firewall 140. In one embodiment, the real-time packets 152 may include real-time media information such as Voice over IP (VoIP), video, or audio/video. The call server 130 is a computer system that contains database, storage, processing power, switch and connection interfaces to other elements in the network 110. The call server 130 communicates with the end system 120 for a call setup, either during receiving and transmitting, using a call setup protocol 125. In addition, the call server 130 communicates with the firewall 140 using a control protocol 135.

The private network 170 is a network internal to the organization, e.g., an intranet. The private network 170 includes an end system 180 and a call server 190. The end system 180 is a system that receives or transmits a call or a message. Examples of the end system 180 include a computer, a processor, a central processing unit, a digital signal processing system, a call processing unit, a workstation, a private branch exchange (PBX), a telephony device, a wireless call unit, etc. The end system 180 sends or receives real-time packets 154 to or from the firewall 140. In one embodiment, the real-time packets 154 may include real-time media information such as Voice over IP (VoIP), video, or audio/video. The call server 190 is a computer system that contains database, storage, processing

power, switch and connection interfaces to other elements in the network 170. The call server 190 communicates with the end system 180 for a call setup, either during receiving and transmitting, using a call setup protocol 185. In addition, the call server 190 communicates with the firewall 140 using a control protocol 195.

At any time, the public network 110 may be transmitting or receiving a call to or from the network 170 via the firewall 140. Similarly, the private network 170 may be transmitting or receiving a call to or from the public network 110 via the firewall 140. A network that is transmitting information is a source network and a network that is receiving information is a destination network.

The firewall 140 is located between the networks 110 and 170. The firewall 140 includes a real-time firewall 150 and an application firewall 160. Each of the firewalls 150 and 160 can also perform network address translation (NAT). In one embodiment, packets go to the real-time firewall 150 first. The real-time firewall 150 receives real-time packets from the source network and forwards packets that are accepted according to some filtering characteristics described in the corresponding control protocol. Packets that are rejected are then forwarded to the application firewall 160 or discarded or dumped. The application firewall 160 can apply more complex analysis such as stateful inspection to determine if the packets should be allowed in or out.

Figure 2 is a diagram illustrating the real-time firewall 150 shown in Figure 1 according to one embodiment of the invention. The real-time firewall 150 includes a controller 210, a filter 230, and a modifier 250. The controller 210, the filter 230, and the modifier 250 may be implemented by hardware, software, firmware or any combination thereof. Hardware, software, or firmware implementation may be represented by modules. Module coupling may include physical connections, common memory, message passing, parameter and/or argument passing, or any technique that allows information from one module to be transferred to another module.

The controller 210 specifies a filtering characteristic 215 based on the control protocol 135 or 195 from the call server 130 or 190. The call server 130 or 190 is shown in Figure 1 and is used to serve the firewall 140 between the

networks 110 and 170. At any time, one of the networks 110 and 170 is a source network and the other is a destination network. The controller 210 further specifies a modifying action 255 based on the control protocol 135 or 195.

The filtering characteristic 215 characterizes the packets to be received or transmitted from the end system 120 or 180 (Figure 1). The filtering characteristic 215 may be any one of a traffic characteristic, a network address, a port identifier, any combination of source and destination addresses and port numbers, or packet fields such as the presence of an RTP header, corresponding to the call at the end system 120 or 180. The call may be a voice over Internet protocol (VoIP) call, a video message, or a video/audio message.

The filter 230 is coupled to the controller 210 to filter the packet 152 or 154 in a call transmitted from the source network based on the filtering characteristic 215. The filter 230 includes an extractor 232, a matcher 234, and a packet router 236. The extractor 232 extracts a characteristic of the packet 152 or 154. The matcher 234 compares the extracted characteristic and the filtering characteristic 215 and generates a matching result. The packet router 236 routes the packet 152/154 to the modifier 250 as an accepted packet 260 if the packet 152/154 satisfies the filtering characteristic 215 (e.g., the matcher 234 generates a matching result between the extracted characteristic and the filtering characteristic 215). The packet router 236 routes the packet 152/154 to the application firewall 160 or merely dumps the packet as a rejected packet 270 if the packet 152/154 does not satisfy the filtering characteristic 215 (e.g., the matcher 234 generates a non-matching result between the extracted characteristic and the filtering characteristic 215). The rejected packet 270 may be further processed by the application firewall 160 to determine if the packet can be further accepted or rejected by the firewall.

The modifier 250 is coupled to the controller 210 and the filter 230 to modify the accepted packet 260 based on the modifying action 255. Then the modified packet is sent to the destination network. The modifying action 255 may be one of an address swapping, a port swapping, a network address translation (NAT), and a protocol conversion. The protocol conversion may be a conversion

from Internet Protocol version 4 (IPv4) to Internet Protocol version 6 (IPv6), or vice versa.

The control protocol 135/195 may be any appropriate protocol. Examples of the control protocol 135/195 include Media Gateway Control (Megaco) protocol and the Common Open Policy Service (COPS) protocol, especially the COPS for Policy Provisioning (COPS-PR).

The COPS is supported at many routers and by policy servers. The COPS messages are transported over a secure TCP connection. The COPS message sequence typically consists of a request (REQ) message and a decision (DEC) message. The REQ message is sent from the real-time firewall 150 to the call server 130/190 to request filtering information. The DEC message is sent from the call server 130/190 to the real-time firewall 150 to contain filtering information including the filtering characteristic 215. The objects carried in the COPS message may include Policy Rule Identifier (PRID) objects, Encoded Policy Instance Data (EPD) objects, and optional extensions. The PRID objects reference one or more specific filtering rules (e.g., traffic bandwidth, IP address or port number corresponding to the call). The EPD objects carry an encoded value comprising a policy or a filtering rule. The extensions may include information on network address translation (NAT) or protocol conversion (e.g., between IPv4 and IPv6).

Figure 3 is a flowchart illustrating a process 300 for real-time media communication across firewall according to one embodiment of the invention. Note that the order of the processing blocks is merely for illustrative purposes. The order of operations may be changed as appropriate.

Upon START, the user initiates a call at the end system (Block 310). This call may include a VoIP, a video message, a video/audio message, or any media message or communication. Then, the end system contacts the corresponding call server to get authorization to make the call according to the call setup protocol (Block 315). Next, the call server downloads the filtering information, including a filtering characteristic, and/or modifying action to the real-time firewall using a control protocol (Block 320). The call server then authorizes the end system to

begin sending real-time packets for the call (Block 325). Upon receipt of the authorization from the call server, the end system sends real-time packets to the real-time firewall (Block 330). Then, the filter in the real-time firewall checks the packets against the filtering characteristic and other criteria (Block 335).

Next, it is determined if the packet matches the filtering characteristic (Block 340). If not, the packet is rejected and is forwarded to the application firewall or is discarded (Block 345). The process 300 is then terminated. Otherwise, if the packet satisfies the filtering characteristic, it is accepted and is forwarded to the modifier (Block 350). Then, the modifier optionally adds a modifying action (e.g., swap addresses, swap port numbers, convert protocol) to the accepted packet (Block 355). The modifier then forwards the modified packet to the destination network (Block 360). The process 300 is then permitted.

While this invention has been described with reference to illustrative embodiments, this description is not intended to be construed in a limiting sense. Various modifications of the illustrative embodiments, as well as other embodiments of the invention, which are apparent to persons skilled in the art to which the invention pertains are deemed to lie within the spirit and scope of the invention.

CLAIMS

What is claimed is:

1. An apparatus comprising:

a controller to specify a filtering characteristic based on a control protocol from a call server serving a firewall between a source and a destination networks; and

a filter coupled to the controller to filter a packet in a call transmitted from the source network based on the filtering characteristic, the filter accepting the packet if the packet satisfies the filtering characteristic and rejecting the packet otherwise.

2. The apparatus of claim 1 wherein the controller further specifies a modifying action based on the control protocol.

3. The apparatus of claim 2 further comprises:

a modifier coupled to the controller and the filter to modify the accepted packet based on the modifying action, the modified packet being sent to the destination network.

4. The apparatus of claim 1 wherein the source network is one of a public network and a private network.

5. The apparatus of claim 1 wherein the destination network is one of a public network and a private network.

6. The apparatus of claim 1 wherein the filtering characteristic is one of a traffic characteristic, a network address, and a port identifier corresponding to the call.

7. The apparatus of claim 1 wherein the rejected packet is sent to an application firewall.

8. The apparatus of claim 3 wherein the modifying action is one of an address swapping, a port swapping, and a protocol conversion.

9. The apparatus of claim 8 wherein the protocol conversion is a conversion between an IPv4 and an IPv6.

10. The apparatus of claim 6 wherein the call is a voice over Internet protocol (VoIP) call.

11. The apparatus of claim 1 wherein the control protocol is one of a megaco protocol and a Common Open Policy Service (COPS) protocol.

12. The apparatus of claim 1 wherein the filter comprises:

an extractor to extract a packet characteristic from the packet;

a matcher coupled to the extractor to match the packet characteristic with the filtering characteristic; and

a packet router coupled to the matcher to route the packet to the modifier if the packet characteristic matches the filtering characteristic.

13. A method comprising:

specifying a filtering characteristic based on a control protocol from a call server serving a firewall between a source and a destination networks;

filtering a packet in a call transmitted from the source network based on the filtering characteristic; and

accepting the packet if the packet satisfies the filtering characteristic and rejecting the packet otherwise.

14. The method of claim 13 wherein specifying further comprises specifying a modifying action based on the control protocol.

15. The method of claim 14 further comprises:

modifying the accepted packet based on the modifying action, the modified packet being sent to the destination network.

16. The method of claim 13 wherein the source network is one of a public network and a private network.

17. The method of claim 13 wherein the destination network is one of a public network and a private network.

18. The method of claim 13 wherein the filtering characteristic is one of a traffic characteristic, a network address, and a port identifier corresponding to the call.

19. The method of claim 13 wherein the rejected packet is sent to an application firewall.

20. The method of 13 wherein the modifying action is one of an address swapping, a port swapping, and a protocol conversion.

21. The method of claim 20 wherein the protocol conversion is a conversion between an IPv4 and an IPv6.

22. The method of claim 18 wherein the call is a voice over Internet protocol (VoIP) call.

23. The method of claim 13 wherein the control protocol is one of a megaco protocol and a Common Open Policy Service (COPS) protocol.

24. The method of claim 13 wherein filtering comprises:

extracting a packet characteristic from the packet;

matching the packet characteristic with the filtering characteristic; and

routing the packet to the modifier if the packet characteristic matches the filtering characteristic.

25. A computer program product comprising:

a machine useable medium having computer program code embedded therein, the computer program product having:

computer readable program code to specify a filtering characteristic based on a control protocol from a call server serving a firewall between a source and a destination networks; and

computer readable program code to filter a packet in a call transmitted from the source network based on the filtering characteristic; and

computer readable program code to accept the packet if the packet satisfies the filtering characteristic and rejecting the packet otherwise.

26. The computer program product of claim 25 wherein the computer readable program code to specify further comprises specifying a modifying action based on the control protocol.

27. The computer program product of claim 26 further comprises:

computer readable program code to modify the accepted packet based on the modifying action, the modified packet being sent to the destination network.

28. The computer program product of claim 25 wherein the source network is one of a public network and a private network.

29. The computer program product of claim 25 wherein the destination network is one of a public network and a private network.

30. The computer program product of claim 25 wherein the filtering characteristic is one of a traffic characteristic, a network address, and a port identifier corresponding to the call.

31. The computer program product of claim 25 wherein the rejected packet is sent to an application firewall.

32. The computer program product of 25 wherein the modifying action is one of an address swapping, a port swapping, and a protocol conversion.

33. The computer program product of claim 32 wherein the protocol conversion is a conversion between an IPv4 and an IPv6.

34. The computer program product of claim 30 wherein the call is a voice over Internet protocol (VoIP) call.

35. The computer program product of claim 25 wherein the control protocol is one of a megaco protocol and a Common Open Policy Service (COPS) protocol.

36. The computer program product of claim 25 wherein the computer readable program code to filter comprises:

computer readable program code to extract a packet characteristic from the packet;

computer readable program code to match the packet characteristic with the filtering characteristic; and

computer readable program code to route the packet to the modifier if the packet characteristic matches the filtering characteristic.

37. A system comprising:

a source and destination networks;

an application firewall coupled to the source and destination networks; and

a real-time firewall coupled to the source and destination networks to process real-time packets, the real-time firewall comprising:

a controller to specify a filtering characteristic based on a control protocol from a call server serving a firewall between a source and a destination networks, and

a filter coupled to the controller to filter a packet in a call transmitted from the source network based on the filtering characteristic, the filter accepting the packet if the packet satisfies the filtering characteristic and rejecting the packet otherwise.

38. The system of claim 37 wherein the controller further specifies a modifying action based on the control protocol.

39. The system of claim 38 further comprises:

a modifier coupled to the controller and the filter to modify the accepted packet based on the modifying action, the modified packet being sent to the destination network.

40. The system of claim 37 wherein the source network is one of a public network and a private network.

41. The system of claim 37 wherein the destination network is one of a public network and a private network.

42. The system of claim 37 wherein the filtering characteristic is one of a traffic characteristic, a network address, and a port identifier corresponding to the call.

43. The system of claim 37 wherein the rejected packet is sent to an application firewall.

44. The system of claim 39 wherein the modifying action is one of an address swapping, a port swapping, and a protocol conversion.

45. The system of claim 44 wherein the protocol conversion is a conversion between an IPv4 and an IPv6.

46. The system of claim 42 wherein the call is a voice over Internet protocol (VoIP) call.

47. The system of claim 37 wherein the control protocol is one of a megaco protocol and a Common Open Policy Service (COPS) protocol.

48. The system of claim 37 wherein the filter comprises:

an extractor to extract a packet characteristic from the packet;

a matcher coupled to the extractor to match the packet characteristic with the filtering characteristic; and

a packet router coupled to the matcher to route the packet to the modifier if the packet characteristic matches the filtering characteristic.

49. An apparatus comprising:

a controller to specify a filtering characteristic based on a control protocol from a call server serving a firewall between a source and a destination networks;

a filter coupled to the controller to filter a packet in a call transmitted from the source network based on the filtering characteristic, the filter accepting the packet if the packet satisfies the filtering characteristic and rejecting the packet otherwise; and

a modifier coupled to the controller and the filter to modify the accepted packet based on the modifying action, the modified packet being sent to the destination network.

50. The apparatus of Claim 49 wherein the controller further specifies a modifying action based on the control protocol.

51. The apparatus of claim 1 wherein the source network is one of a public network and a private network.

52. The apparatus of claim 1 wherein the destination network is one of a public network and a private network.

ABSTRACT OF THE DISCLOSURE

In one embodiment of the invention, a real-time firewall processor includes a controller and a filter. The controller specifies a filtering characteristic based on a control protocol from a call server serving a firewall between a source and a destination networks. The filter is coupled to the controller to filter a packet in a call transmitted from the source network based on the filtering characteristic, the filter accepting the packet if the packet satisfies the filtering characteristic and rejecting the packet otherwise.

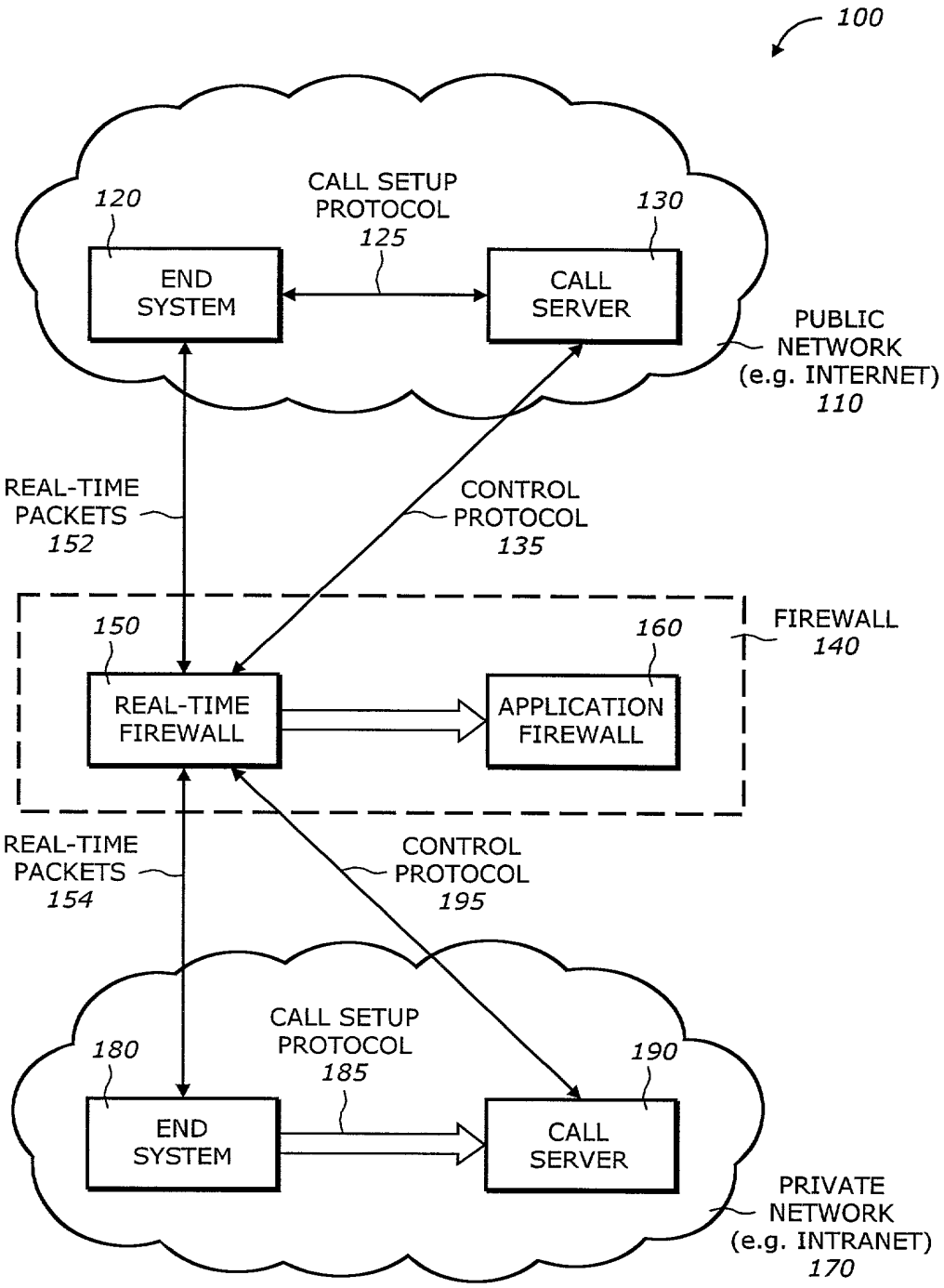
100
CALL SETUP PROTOCOL
125
120
130
END SYSTEM
CALL SERVER
PUBLIC NETWORK (e.g. INTERNET)
110
REAL-TIME PACKETS
152
CONTROL PROTOCOL
135
FIREWALL
140
150
160
REAL-TIME FIREWALL
APPLICATION FIREWALL
REAL-TIME PACKETS
154
CONTROL PROTOCOL
195
CALL SETUP PROTOCOL
185
180
190
END SYSTEM
CALL SERVER
PRIVATE NETWORK (e.g. INTRANET)
170

FIG. 1

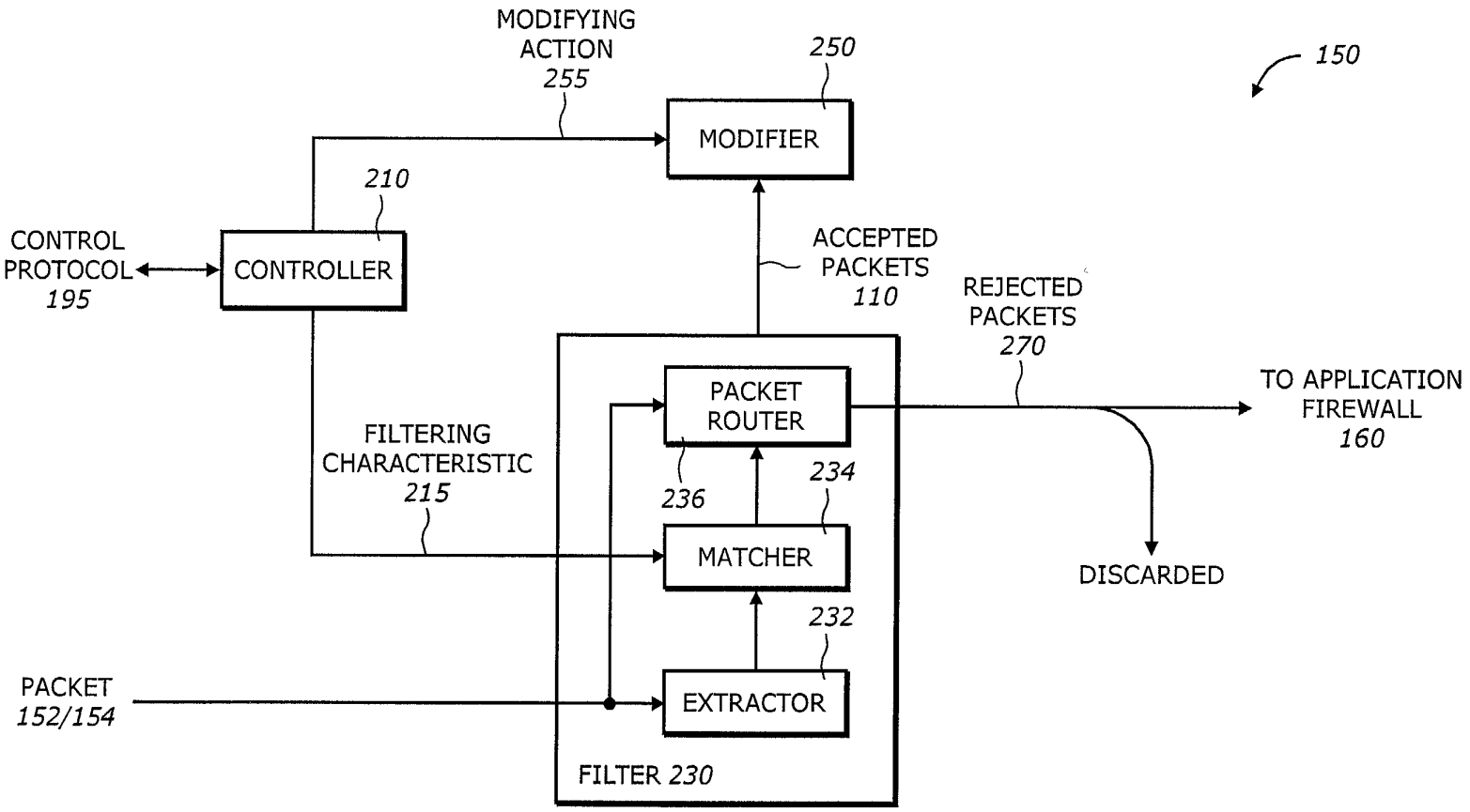
MODIFYING ACTION 255
250
150
MODIFIER
210
CONTROL PROTOCOL 195
CONTROLLER
ACCEPTED PACKETS 110
REJECTED PACKETS 270
TO APPLICATION FIREWALL 160
PACKET ROUTER
FILTERING CHARACTERISTIC 215
236
234
MATCHER
DISCARDED
232
PACKET 152/154
EXTRACTOR
FILTER 230

FIG. 2

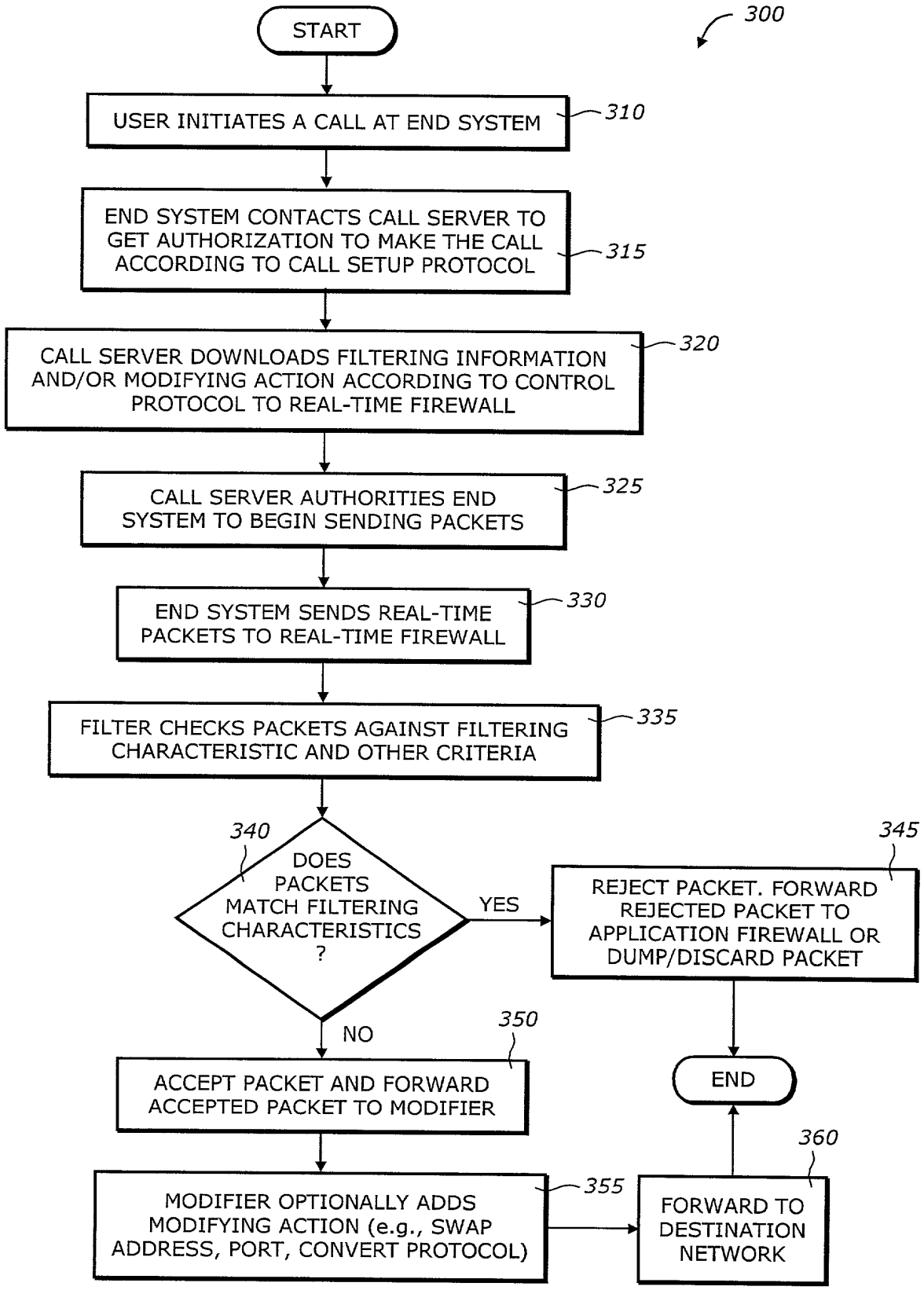
300
START
USER INITIATES A CALL AT END SYSTEM
310
END SYSTEM CONTACTS CALL SERVER TO GET AUTHORIZATION TO MAKE THE CALL ACCORDING TO CALL SETUP PROTOCOL
315
CALL SERVER DOWNLOADS FILTERING INFORMATION AND/OR MODIFYING ACTION ACCORDING TO CONTROL PROTOCOL TO REAL-TIME FIREWALL
320
CALL SERVER AUTHORITIES END SYSTEM TO BEGIN SENDING PACKETS
325
END SYSTEM SENDS REAL-TIME PACKETS TO REAL-TIME FIREWALL
330
FILTER CHECKS PACKETS AGAINST FILTERING CHARACTERISTIC AND OTHER CRITERIA
335
340
DOES PACKETS MATCH FILTERING CHARACTERISTICS ?
YES
345
REJECT PACKET. FORWARD REJECTED PACKET TO APPLICATION FIREWALL OR DUMP/DISCARD PACKET
NO
350
ACCEPT PACKET AND FORWARD ACCEPTED PACKET TO MODIFIER
END
360
MODIFIER OPTIONALLY ADDS MODIFYING ACTION (e.g., SWAP ADDRESS, PORT, CONVERT PROTOCOL)
355
FORWARD TO DESTINATION NETWORK

FIG. 3

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below, next to my name.

I believe I am the original, first, and sole inventor (if only one name is listed below) or an original, first, and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

Real-Time Media Communication Over Firewalls Using a Control Protocol

the specification of which

[X] is attached hereto.

[ ] was filed on _____ as
United States Application Number _____
or PCT International Application Number _____
and was amended on _____
(if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment referred to above. I do not know and do not believe that the claimed invention was ever known or used in the United States of America before my invention thereof, or patented or described in any printed publication in any country before my invention thereof or more than one year prior to this application, that the same was not in public use or on sale in the United States of America more than one year prior to this application, and that the invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve months (for a utility patent application) or six months (for a design patent application) prior to this application.

I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d), of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s):

APPLICATION NUMBER	COUNTRY (OR INDICATE IF PCT)	DATE OF FILING (day, month, year)	PRIORITY CLAIMED UNDER 37 USC 119
			☐ No ☐ Yes
			☐ No ☐ Yes
			☐ No ☐ Yes

I hereby claim the benefit under Title 35, United States Code, Section 119(e) of any United States provisional application(s) listed below:

APPLICATION NUMBER	FILING DATE

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

APPLICATION NUMBER	FILING DATE	STATUS (ISSUED, PENDING, ABANDONED)

I hereby appoint the persons listed on Appendix A hereto (which is incorporated by reference and a part of this document) as my respective patent attorneys and patent agents, with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.

Send correspondence to:
Thinh V. Nguyen, Reg. No. 42,034, BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN, LLP
(Name of Attorney or Agent)
12400 Wilshire Boulevard, 7th Floor, Los Angeles, California 90025 and direct telephone calls to:
Thinh V. Nguyen, (714) 557-3800.
(Name of Attorney or Agent)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Sole/First Inventor (given name, family name) **Lyndon Ong**

Inventor's Signature Lyndon Ong Date 10/31/00

Residence San Jose, California USA Citizenship USA
(City, State) (Country)

P. O. Address 5 10 4716 Mill River Lane

San Jose, California 95134 USA

APPENDIX A

I hereby appoint BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP, a firm including: William E. Alford, Reg. No. 37,764; Farzad E. Amini, Reg. No. 42,261; William Thomas Babbitt, Reg. No. 39,591; Carol F. Barry, Reg. No. 41,600; Jordan Michael Becker, Reg. No. 39,602; Lisa N. Benado, Reg. No. 39,995; Bradley J. Bereznak, Reg. No. 33,474; Michael A. Bernadicou, Reg. No. 35,934; Roger W. Blakely, Jr., Reg. No. 25,831; R. Alan Burnett, Reg. No. 46,149; Gregory D. Caldwell, Reg. No. 39,926; Andrew C. Chen, Reg. No. 43,544; Thomas M. Coester, Reg. No. 39,637; Donna Jo Coningsby, Reg. No. 41,684; Florin Corie, Reg. No. 46,244; Dennis M. deGuzman, Reg. No. 41,702; Stephen M. De Klerk, Reg. No. P46,503; Michael Anthony DeSanctis, Reg. No. 39,957; Daniel M. De Vos, Reg. No. 37,813; Sanjeet Dutta, Reg. No. P46,145; Matthew C. Fagan, Reg. No. 37,542; Tarek N. Fahmi, Reg. No. 41,402; George Fountain, Reg. No. 36,374; Paramita Ghosh, Reg. No. 42,806; James Y. Go, Reg. No. 40,621; James A. Henry, Reg. No. 41,064; Willmore F. Holbrow III, Reg. No. P41,845; Sheryl Sue Holloway, Reg. No. 37,850; George W Hoover II, Reg. No. 32,992; Eric S. Hyman, Reg. No. 30,139; William W. Kidd, Reg. No. 31,772; Sang Hui Kim, Reg. No. 40,450; Walter T. Kim, Reg. No. 42,731; Eric T. King, Reg. No. 44,188; Erica W. Kuo, Reg. No. 42,775; George B. Leavell, Reg. No. 45,436; Gordon R. Lindeen III, Reg. No. 33,192; Jan Carol Little, Reg. No. 41,181; Kurt P. Leyendecker, Reg. No. 42,799; Joseph Lutz, Reg. No. 43,765; Michael J. Mallie, Reg. No. 36,591; Andre L. Marais, under 37 C.F.R. § 10.9(b); Paul A. Mendonsa, Reg. No. 42,879; Clive D. Menezes, Reg. No. 45,493; Chun M. Ng, Reg. No. 36,878; Thien T. Nguyen, Reg. No. 43,835; Thinh V. Nguyen, Reg. No. 42,034; Dennis A. Nicholls, Reg. No. 42,036; Daniel E. Ovanezian, Reg. No. 41,236; Kenneth B. Paley, Reg. No. 38,989; Marina Portnova, Reg. No. P45,750; William F. Ryann, Reg. 44,313; James H. Salter, Reg. No. 35,668; William W. Schaal, Reg. No. 39,018; James C. Scheller, Reg. No. 31,195; Jeffrey Sam Smith, Reg. No. 39,377; Maria McCormack Sobrino, Reg. No. 31,639; Stanley W. Sokoloff, Reg. No. 25,128; Judith A. Szepesi, Reg. No. 39,393; Vincent P. Tassinari, Reg. No. 42,179; Edwin H. Taylor, Reg. No. 25,129; John F. Travis, Reg. No. 43,203; Joseph A. Twarowski, Reg. No. 42,191; Thomas A. Van Zandt, Reg. No. 43,219; Lester J. Vincent, Reg. No. 31,460; Glenn E. Von Tersch, Reg. No. 41,364; John Patrick Ward, Reg. No. 40,216; Mark L. Watson, Reg. No. P46,322; Thomas C. Webster, Reg. No. P46,154; and Norman Zafman, Reg. No. 26,250; my patent attorneys, and Firasat Ali, Reg. No. 45,715; and Justin M. Dillon, Reg. No. 42,486; Raul Martinez, Reg. No. 46,904; my patent agents, with offices located at 12400 Wilshire Boulevard, 7th Floor, Los Angeles, California 90025, telephone (714) 557-3800, and Holmes W. Anderson, Reg. No. 37,272; Christopher J. Cianciolo, Reg. No. 42,417; John D. Crane, Reg. No. 25,231; John C. Gorecki, Reg. No. 38,471; Howard R. Greenberg, Reg. No. 26,171; W. Glen Johnson, Reg. No. 39,525; Lindsay G. McGuinness, Reg. No. 38,549; Jeffrey M. Measures, Reg. No. 40,272; Randall Mishler, Reg. No. 42,006; Kevin L. Smith, Reg. No. 38,620; Mary M. Steubing, Reg. No. 37,946; and Vernon E. Williams, Reg. No. 38,713 of NORTEL NETWORKS LIMITED with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.